IBIA

International Biometric Industry Association

Statement of
Martin Huddart

Chairman of the Board
International Biometric Industry Association

Before the
Subcommittee on Aviation
Committee on Transportation and Infrastructure
U.S. House of Representatives

May 19, 2004

Mr. Chairman and members of the subcommittee, thank you for inviting the biometric industry to offer its views at this important proceeding. My name is Martin Huddart. I am the Vice President of Business Development for the Electronic Access and Biometric Groups at Ingersoll-Rand. Recognition Systems, Inc., a subsidiary of Ingersoll-Rand, is the developer and manufacturer of a hand geometry biometric system and also offers fingerprint biometric solutions.

I am also Chairman of the Board of Directors of the International Biometric Industry Association (IBIA), and I represent IBIA here today. IBIA was founded in 1998 and is headquartered in Washington, D.C. IBIA's members are leading developers, manufacturers, and integrators of the full range of biometric technologies.

Overview about Biometrics. Biometrics are technologies that automatically identify or verify the identity of an individual by measuring physiological or behavioral characteristics. This authentication of identity is accomplished by using computer technology in a noninvasive way to match patterns of live individuals in real time against enrolled records. Examples of the patterns used for biometric identification include those made from the image of a fingerprint, the geometry of the hand, and unique patterns in a person's iris, voice, signature, or face. It is important to know that most biometric applications do not store the actual image of the feature being measured. Instead, the measurements are converted into a biometric file which is generally encrypted. Without the key to unlock the encryption, a biometric file cannot be reverse engineered to determine a person's name, age, sex, race or any other personal information. Likewise, it cannot be abused to steal someone's identity. In short, biometrics, properly used, protect privacy.

Biometrics are the only technologies that offer an effective response to the need for automated personal authentication as an essential component of strong homeland security systems without sacrificing convenience. The U.S. government was an early adopter of biometrics, first using the technologies to control access to highly sensitive facilities such as nuclear power plants and weapons storage locations. Now, use of biometrics is expanding to protect networks against intrusion by hackers, to secure records from identity theft, to ensure that benefits are disbursed to lawful recipients, and – not least – to protect international borders.

Continuing Threats to Aviation. Government and private industry have recognized the need for systems of positive personal identification – specifically by deploying biometrics – since 9/11. It is now widely acknowledged that terrorism, and indeed all criminal activity, thrives in an atmosphere of anonymity and false identity. The crucial issue is balancing the necessity for positive identification with our desires for a free and open society. Freedom to travel, a treasured benefit in our democracy, is exploited and corrupted by those who would threaten all movement, all travel, thus creating the appearance of imminent danger in the attempt to impose fear on our population and cripple the economy. We need to deny them that opportunity without sacrificing our rights of travel.

Many efforts have been made since 9/11 to address the need for additional security through biometrics in the aviation environment. Most were well-intended and necessary initial steps to improve air travelers' security, but they have also been piecemeal, hurried, and reactive. Accordingly, this statement by IBIA addresses remaining gaps in aviation security that can be filled by biometrics in order to help create a well-designed and comprehensive deterrent against terrorism in the aviation sector. With proper care, IBIA's recommendations to improve aviation security can also be leveraged to create striking improvements in passenger convenience and airline productivity that will help revitalize the aviation industry and encourage expanded travel and tourism.

Required Upgrades of Employee Identification to Strengthen Physical Access Controls. On May 7, 2004 TSA issued a Request for Proposal (RFP) for the Transportation Worker Identification Credential (TWIC). The RFP is the result of extensive consultation with industry by TSA, and it serves as the central guideline for employee identification in order to strengthen physical access controls for air, sea, and land transport workers. The RPF makes clear that TSA has considered an end-to-end solution. First, biometrics will be collected and enrolled to establish the identity of transport workers. After a background check by TSA, transport workers will be issued a credential that will hold a biometric. Workers' biometrics will also be retained in computer systems for future re-issuance in cases of lost or stolen credentials. Finally the TWIC system will use the biometric stored on the credential to integrate identity management and access control in local systems at airports, seaports, rail, pipeline, trucking and mass transit facilities.

The TWIC identification system will add needed clarity to the current TSA regulation governing the security of sensitive areas of airports. The current regulation reads as follows:

> "(a) Secured area. Except as provided in paragraph (b) of this section, the measures for controlling entry to the secured area required under §1542.201(b)(1) must:
>
> (1) Ensure that only those individuals authorized to have unescorted access to the secured area are able to gain entry;"

Biometrics are not stipulated in this regulation but – as the TWIC RFP recognizes -- biometrics in fact are the only secure way to authorize personal access in sensitive areas of airports. Most airports currently address the current TSA regulation by requiring personnel to swipe a card through a reader and enter a personal identification number (PIN). This system has wholesale vulnerabilities. Cards authorize access not to persons but only to pieces of plastic that are subject to loss, theft, or copying. Recently, a Category X airport – which includes the largest U.S. airports -- admitted that its annual identification badge loss exceeded 400 per year, a very large number. By contrast, airport personnel enrolled in biometric systems cannot transfer their identity to someone else, and their biometric information cannot be borrowed and used by an unauthorized party. Moreover, advanced versions of biometric access control systems combine the technology with sophisticated software that can limit users to certain airport doorways at certain times, and can track who accesses which door at what time.

Hand geometry is in use, for example, in airports at San Francisco, Nevada, and Toledo. An additional 15 U.S. airports are conducting trials of hand geometry at single entry points. Fingerprint controls are in use at Little Rock, Arkansas and Chicago O'Hare. Iris technology has been deployed at Terminal 4, the international arrivals terminal, at JFK Airport in New York.

These are rare exceptions, however. Many other airports are delaying a decision to deploy biometrics until the completion of testing of "new and emerging security technologies." These tests, being conducted at 20 airports, were mandated by the Aviation Security Act of November 2001. The law also provides that the Under Secretary for Transportation Security "shall review the effectiveness of biometrics systems currently in use at several United States airports."

The test process appears to be preoccupied with "new and emerging" technologies at the expense of deployed, proven technologies. For example, none of the first eight airports in the test uses hand geometry, which has proved its effectiveness in airport deployments that predate 9/11. Thus far the test managers have not reviewed the effectiveness of any operational biometric system already in place at an airport. It is not clear why. The test managers themselves say that in the end they will not recommend any biometric over any other and airports will be able to choose among proven biometric systems, yet the conclusion of the current test process appears to be at least a year away.

This long delay is unnecessary. Any of several biometrics that have proved their effectiveness in years of airport deployment could be approved for deployment today at all U.S. airports. Other biometrics could be approved later when tests demonstrate their effectiveness. Moreover, at least part of the funds being expended in the overly prolonged test process could be used for actual biometric deployment. My own calculation is that the money allocated to the test process could have retrofitted approximately 45 of the top 200 airports with biometrics.

The TWIC system has been structured to accommodate multiple biometrics, and it requires no more delay in the "testing" process. It is long past time to strengthen physical access control of personnel at airports by deploying biometrics properly for personal identification.

Improvements Needed to Identify Air Travelers. In the same way that TSA has adopted a comprehensive approach to airport security through TWIC, TSA must also adopt a comprehensive and holistic "registered traveler program." Post-9/11 security requirements have made air travel less convenient but only minimally safer. Deploying biometrics to positively identify travelers using a voluntary system could improve air travel security and convenience.

On April 5, Rear Admiral David M. Stone, Acting Administrator of the Transportation Security Administration (TSA), announced that the agency is seeking responses from the private sector to an RFP for a Registered Traveler (RT) Pilot Program that will begin in select airports in late June.

The RT Pilot will use biometrics to enhance security and efficiency. It is intended to create an information technology system that will fully integrate biometric identification with the results of security assessments to ensure fast, secure, and reliable personal identification and reliable measures of security status at airport checkpoints. The RT Pilot Program will ask volunteers to submit information, including biometrics, necessary for TSA to determine eligibility. The biometric information will be used to verify identity and in conjunction with a security assessment will allow passengers to pass through an expedited airport security screening process. All volunteers will continue to undergo basic physical screening procedures.

Biometric technologies have demonstrated their ability to eliminate bottlenecks in secured processing environments. The clearest example of this capability is in border control. Biometrics have been used in the most sensitive national security applications to routinely admit pre-registered border crossers. One of the best examples is the Israeli-Palestinian border project. Palestinians daily enter and exit Israel in order to conduct their business, visit families, and work in Israel. The 40,000 workers arriving daily from Gaza need to enter Israel within a three-hour period and exit at the end of the working day. A manual check would require hundreds of persons to man security checkpoints without a guarantee of reliability. By using biometrics, people entering or exiting Israel can be verified or rejected within seconds.

Palestinians wishing to enter Israel are issued a highly secure smart card after first enrolling in the system, receiving clearance that they have no previous terrorist or criminal record and that they have not previously enrolled in the system under an alias. The smart card holds substantial information, including biometric templates and personal and security data.

A Palestinian wishing to legitimately enter or exit Israel at a border crossing checkpoint presents a smart card at a biometric kiosk then places his or her hand on a reader, is biometrically verified as claimed, and after being cleared, proceeds through an open gate. Biometrics thus allow Israel to automatically verify a person's identity in the shortest possible time, in a user-friendly way, while maintaining a high level of security.

The Israeli-Palestinian border project is a prototype of how the TSA Registered Traveler program might work to ease air travel bottlenecks and simultaneously strengthen security.

Essential Changes in Credentialing of Law Enforcement Officers Carrying Weapons. Verifying the identity of authorized law enforcement officers who carry firearms onto planes is not a new issue but it remains a matter of real vulnerability. The issue arose well before 9/11 but has gained greater salience since then.

Credentials presented by law enforcement officers differ greatly but they are as unreliable as drivers' licenses to verify identity and they suffer from the same inherent problems of insecurity. Law enforcement officers' credentials typically consist of documents containing descriptions, photographs, and/or signatures. It is thoroughly insecure to try to verify personal identity by relying upon descriptions, photos, or signatures that are neither intended nor designed to be an integral component of an automated biometric identification system. A process this insecure is an open invitation to criminal and terrorist deception.

The General Services Administration and some state governments have begun to issue credentials (badges, drivers' licenses, and entitlement benefit cards, for example) that include an encrypted biometric template, but most government identification documents currently include no biometric. A digital photo standing alone, commonly used on identification credentials, is a wholly inadequate means of personal identification. Without standardized biometric authentication, attempts to use photos to achieve a valid 1:1 match is equivalent to the "garbage in, garbage out" aphorism often suggested by computer programmers.

To be acceptable, a law enforcement officer's credential presented to a TSA official must prove that the bearer is who he or she claims to be. For the same reason that biometrics are essential to authenticate the personal identity of transport workers and airline passengers, biometrics are required to prove the identity of law enforcement officers. Using a biometric 1:1 match to affirm the validity of the credentials held by a law enforcement officer is indispensable to helping deter the use of stolen or forged documents by criminals or terrorists posing as law enforcement officers.

Standards for Biometric Implementation at Airports and for Interoperability. Operational standards to implement biometrics at airports are being defined by both the TWIC program and the Registered Traveler program. Both will need to be further refined as the systems are deployed. In addition, the US-VISIT program is setting standards for air passenger security. These programs will help define operational guidelines to protect airports and air travelers. In addition, the biometric industry is hard at work to define standards for interoperability.

Notably, the biometric industry and government have worked together to develop a set of rules about how biometrics are to be integrated into computer operating systems. This is an exceptionally important advancement for several reasons:

- It accommodates multiple biometrics.
- It allows the quick adoption of new biometric technologies as they are deployed.
- It permits the rapid exchange of information for record checks.
- It enables users to voluntarily share biometric information that has been acquired by other sources, such as employers, airlines, and government agencies.

It is sometimes said that "the biometric industry has no standards." The statement is not accurate, but there is confusion about the alphabet soup of biometric standards initiatives under way domestically and internationally.

In fact considerable progress has been achieved. The BioAPI Consortium, a voluntary initiative driven by the U.S. biometric industry, is far along in balloting a base interoperability standard for biometrics through the International Organization for Standardization (ISO). The BioAPI, or Biometric Application Programming Interface, already serves as the cornerstone for interoperability in the Federal government. GSA, TSA, and the Department of Defense's Biometric Management Office require compliance with BioAPI as a condition of Federal government procurement of biometrics.

Beyond the initiative to achieve a base interoperability standard, standards initiatives in particular applications are proceeding through the American National Standards Institute (ANSI), through ISO working groups, and through the UN-recognized International Civil Aviation Organization (ICAO). These initiatives are developing standards for border crossing documentation – meaning biometrically-enabled passports and visas – for multi-modal biometric interoperability, for smart card and biometric interoperability, and for privacy and template security. The National Biometric Security Project, scheduled to present testimony at the May 19 hearing of the Aviation Subcommittee, is playing a central and vital role in all of these initiatives.

Conclusion. The need to deploy biometrics to help ensure aviation security is no longer a matter of real debate. Rather, the urgent task is to implement a coherent, holistic plan to deploy biometric technologies with all deliberate speed in the applications in which biometrics can clearly strengthen the security of airports and air travel. They include using biometrics:

- To control physical access to sensitive airport facilities.
- To identify airport and airline employees.
- To verify the identity of air travelers.
- To protect against unauthorized carrying of firearms on planes.

IBIA stands ready to support legislation and other initiatives by the Subcommittee on Aviation to advance toward these goals.